UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

v. Case No. 16-CR-103

NEIL C. KIENAST,

Defendant.

DECISION AND ORDER DENYING MOTION TO SUPPRESS

Defendant Neil C. Kienast has been charged in a superseding indictment with two counts of receiving child pornography, in violation of 18 U.S.C. § 2252A(a)(2), and one count of possession of child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). The case is presently before the court on Kienast's motion to suppress the evidence seized from his home and computer pursuant to a search warrant issued by Magistrate Judge James R. Sickel, as well as any evidence derived therefrom. For the reasons that follow, Kienast's motion will be denied.

The charges against Kienast stem from a nationwide child pornography investigation conducted by the FBI in conjunction with the U.S. Department of Justice. Acting in part upon a tip from a foreign law enforcement agency, the FBI was able to seize control of an online forum hosted at a facility in North Carolina which was dedicated to the advertisement and distribution of child pornography, "Website A". Website A had 150,000 members who collectively engaged in tens of thousands of postings of child pornography images and videos categorized according to the gender and age of the minor victim. The site did not advertise or distribute adult pornographic images.

Website A operated as a "hidden service" on the anonymous TOR network and was generally not accessible through the traditional internet. To access Website A, a user had to know its exact web address on the TOR network. In addition, the TOR network allows users to hide their actual IP addresses while accessing the internet. To access the TOR network, a user must install TOR software which routes user communications around a distributed network of relay computers called nodes, which are run by volunteers around the world. When a user on the TOR network accesses a website, the IP address of a TOR "exit node," rather than the user's actual IP address, shows up on the website's IP log. An exit node is the last computer through which the user's communications are routed. TOR is designed to prevent tracing the user's actual IP address back through the TOR exit node IP address. As a result, traditional IP-address-based identification techniques used by law enforcement agents investigating online crimes are not viable against a website operated on the TOR network. NIT Search Warrant (ECF No. 12-3).

Faced with this investigative roadblock, FBI agents took an unusual step. Instead of immediately shutting Website A down, which would have allowed the users of the site to go unidentified and free to continue receiving and trafficking in child pornography, the FBI seized control of Website A and continued it in operation for a two-week period from a facility located in the Eastern District of Virginia. The FBI also obtained a search warrant from a magistrate judge in that District that authorized the agency to use a "Network Investigative Technique" (NIT) to identify individual users who were accessing content on the site. The NIT consisted of computer instructions which were downloaded to the computer of a registered user of Website A, along with the requested content from Website A, when Website A was accessed by such user. Once downloaded, the NIT would cause the user's computer to transmit to the FBI a limited amount of information—the

computer's true IP address and other computer-related information—that would allow the FBI to identify the computer used to access Website A and its user. *Id.*

Based upon data obtained from deployment of the NIT and the logs on Website A, law enforcement learned that a user with the user name "Playpendrifter" actively logged into Website A for a total of 10 hours and 39 minutes between December 9, 2014 and March 4, 2015. On February 25, 2015, Playpendrifter logged into Website A from an IP address of 104.55.29.65 and accessed posts that contained child pornography including a video with 19 images of a prepubescent female between 4 and 6 years of age performing oral sex on an adult male's penis and exposing her vagina and anus. Using publicly available websites, FBI Special Agents were able to determine that the IP address from which Playpendrifter logged into Website A was operated by the Internet Service Provider (ISP) AT&T U-Verse. AT&T U-Verse then provided the FBI with the street address of the premises of the user assigned that IP address in response to an administrative subpoena. That address was the home of Kienast.

Armed with this information, law enforcement agents obtained a warrant authorizing them to search Kienast's residence and seize and examine his computers and related equipment for evidence of the crimes related to child pornography. The warrant was executed on January 16, 2016, and resulted in the seizure of several computers and storage media from Kienast's residence. A subsequent search of the computers revealed child pornography video and image files. Law enforcement also undertook to interview Kienast, and he admitted viewing child pornography for the past several years and using the TOR network to do so. It is this evidence that forms the basis of the charges against him.

Kienast argues that the evidence must be suppressed because the warrant to search his residence is invalid. That warrant is invalid, he contends, because it was obtained using evidence illegally retrieved from his computer via the NIT warrant. Kienast also initially argued that it was also obtained using information illegally obtained from the Social Security Administration (SSA), but he has since abandoned that argument in that whatever evidence law enforcement may have obtained from SSA was not used in its application for the warrant authorizing the search of his home. With respect to the NIT warrant, however, Kienast argues it is void because it was signed by a magistrate judge with no authority to authorize a search outside the boundaries of the district in which her court was located.

Kienast's argument is a technical one based on the language of the statute and rule governing the authority of magistrate judges to issue search warrants. The Federal Magistrates Act provides, in relevant part, as follows:

> (a) Each magistrate judge serving under this chapter shall have *within the district in which sessions are held* by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law—
>
> > (1) all powers and duties conferred or imposed . . . by law or by the Rules of Criminal Procedure for the United States District Courts.

28 U.S.C. § 636(a) (emphasis added). Rule 41(b) of the Federal Rules of Criminal Procedure in turn sets out territorial limits on a magistrate judge's authority to issue a search warrant. It authorizes magistrate judges to issue warrants to (1) "search for and seize a person or property located within [the judge's] district"; (2) search for and seize a person or property located outside the judge's district "if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed"; (3) search for and seize a

person or property located outside the judge's district if the investigation relates to terrorism; (4) install within [the judge's] district a tracking device . . . to track the movement of a person or property located within the district, outside the district, or both; or (5) search for or seize a person or property outside the judge's district but within a United States territory, possession, commonwealth, or premises used by a United States diplomat or consular mission.

Kienast argues that because the NIT was intended to search computers that were outside, as well as inside the Eastern District of Virginia, the magistrate judge in that District acted outside her authority in issuing the NIT warrant. More specifically, he argues that a magistrate judge in Virginia had no authority to authorize a search of his computer in Wisconsin. As a result, Kienast argues that the NIT warrant was void and thus any information obtained from it may not be used against him. And because information obtained from the search authorized by the NIT warrant was used to obtain the Wisconsin warrant that authorized the search of his house and seizure of his computers, Kienast argues that warrant was invalid as well. It thus follows, he contends, that all of the evidence seized from his home based upon that warrant, as well as derivative evidence such as his confession, must be suppressed.

As the defendant notes, the validity of search warrants growing out of the FBI's investigation of Website A based on the NIT warrant has been addressed by courts in districts around the country, including this district. *See United States v. Epich*, 15-CR-163-PP, 2016 WL 953269 (E.D. Wis. Mar. 14, 2016); *see also United States v. Broy*, 16-CR-10030, 2016 WL 5172853, at *1 (C.D. Ill. Sept. 21, 2016) (collecting cases). Though most courts have denied the defendants' motion to suppress, Kienast relies primarily upon the decision in *United States v. Levin*, No. CR 15–10271–WGY, — F.Supp.3d —, 2016 WL 2596010 (D.Mass. May 5, 2016), which did not.

Levin held that because the NIT warrant authorized a search of property outside the territorial jurisdiction of the issuing magistrate judge, it was void *ab initio* and any evidence obtained from its execution was unlawfully obtained. *Levin* further held that the good faith exception to the exclusionary rule set forth in *United State v. Leon*, 468 U.S. 897, 918 (1984), did not apply and thus must be suppressed. Kienast urges this Court to follow *Levin*.

It is the practice in this district that pretrial proceedings, including motions to suppress, are referred to the assigned magistrate judge. On September 7, 2016, Magistrate Judge David E. Jones issued a thorough report recommending that Kienast's motion be denied. Relying on the Seventh Circuit's decision in *United States v. Berkos*, 543 F.3d 392 (7th Cir. 2008), Magistrate Judge Jones found it unnecessary to decide whether the Virginia magistrate judge exceeded her territorial jurisdiction in issuing the NIT warrant and, if so, whether *Leon*'s good faith exception to the exclusionary rule applied. *Berkos* reaffirmed the circuit's previous holdings that "violations of federal rules do not justify the exclusion of evidence that has been seized on the basis of probable cause and with advance judicial approval." *Id.* at 396 (quoting *United States v. Cazares–Olivas*, 515 F.3d 726, 730 (7th Cir.2008); *United States v. Trost*, 152 F.3d 715, 722 (7th Cir.1998)). "The remedy of allowing a defendant to go free based on a violation of Rule 41's requirements for obtaining a proper search warrant," the *Berkos* court noted, "would be 'wildly out of proportion to the wrong.'" *Id.* (quoting *Cazares–Olivas*, 515 F.3d at 730). Noting that the purpose of the exclusionary rule was "to deter illegal police conduct, not mistakes by judges or magistrate judges," Recommendation at 11 (quoting *United States v. Bonner*, 808 F.2d 864, 867 (1st Cir. 1986)), Magistrate Judge Jones concluded that suppression would be especially inappropriate here where "the only mistake law enforcement made . . . was knocking on the wrong door in seeking

authorization for the NIT Warrant." *Id.* at 11 (noting that even *Levin* acknowledged that the NIT Warrant could have been lawfully issued by any of the seven Article III judges routinely sitting in the same courthouse as the issuing magistrate judge). He therefore recommended that Kienast's motion to suppress be denied.

Kienast timely filed his objections to Magistrate Judge Jones' recommendation and requested an evidentiary hearing which the Court held on September 23, 2016. Consistent with his original motion to suppress, Kienast argued in his objections and post hearing brief that, contrary to *Berkos*, suppression of evidence is the proper remedy when law enforcement relies upon a warrant that exceeds the territorial jurisdiction of the issuing magistrate judge. He notes that this case is factually distinguishable from *Berkos* and the cases it relied upon. But, of course, every case is factually distinguishable from every other case. The question is whether the factual distinctions are material such that the principle enunciated by the court in *Berkos* should not apply here. Kienast fails to offer a persuasive argument that the same principle should not apply. Instead, he offers two new arguments that were not properly set forth in his original motion. He argues that the NIT Warrant fails to satisfy the Fourth Amendment's particularity requirement because it "fails to identify in any meaningful way the true scope and nature of the search." Objections at 7. Further, in order to properly establish the scope of the Fourth Amendment violation, Kienast argues he needs the sources for the NIT utilized by the FBI to obtain that identifying information from his computer. Def.'s Offer of Proof (ECF No. 17).

These additional arguments first surfaced in Kienast's reply brief in support of his motion to suppress that he filed before Magistrate Judge Jones. As Magistrate Judge Jones observed, arguments raised for the first time in a reply are deemed waived and need not be addressed.

Recommendation at 6 n.1. (citing *United States v. Diaz*, 533 F.3d 574, 577 (7th Cir. 2008)). But even if they had not been waived, Kienast's new arguments are not persuasive. The thirty-one page affidavit submitted in support of the application for the NIT Warrant in Virginia particularly described the evidence the FBI was seeking—identifying information from the computers of users who were accessing a website exclusively designed to allow the viewing and distribution of child pornography. The facts set forth in the affidavit established at least probable cause, if not virtual certainty, that those accessing the website were committing crimes involving the receipt, possession, and distribution of such material. The particularity requirement is intended "to prevent general searches. By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search is carefully tailored to its justification, and does not resemble the wide-ranging general searches that the Framers intended to prohibit." *Leon*, 468 U.S. at 963 (Stevens, J., dissenting on other grounds). Kienast offers no intelligible argument that the NIT Warrant did not satisfy this requirement. Nor does Kienast offer a persuasive argument why the NIT source code is needed in order to decide his motion. There is no requirement that a warrant specify the precise manner in which the search is to be executed or, in this case, how the NIT actually worked. *Dalia v. United States*, 441 U.S. 238, 257 (1979).

In this case, it is reasonably arguable that the NIT was essentially a tracking device that the Virginia magistrate judge authorized the FBI to install on data retrieved from Website A by users across the country and around the world. The NIT was then carried back to the user's computer with the contraband data and transmitted, much like a traditional tracking device, the address to which it was taken. *See United States v. Jean*, No. 5:15-CR-50087-001, 2016 WL 4771096, at **16– 17 (W.D. Ark. Sept. 13, 2016). If so, then the NIT Warrant was valid and Kienast's motion

could be denied on that basis alone. But even if it did not literally fall within the territorial limits set forth in Rule 41(b), suppression would be entirely inappropriate, especially since the key item of evidence obtained—Kienast's IP address—is not even information over which he would have a reasonable expectation of privacy. *See United States v. Caira*, 833 F.3d 803, 808–09 (7th Cir. 2016) ("Because Caira voluntarily shared his I.P. addresses with Microsoft, he had no reasonable expectation of privacy in those addresses.").

Procedural rules, especially those that protect our homes and persons from unreasonable searches and seizures, are no doubt important, but the investigation and punishment of crime is not a game. It makes no sense to suppress evidence of serious criminal conduct obtained by law enforcement agents operating in good faith on the basis of a warrant issued by a magistrate judge likewise operating in good faith. Suppression of evidence is a drastic remedy that carries heavy costs. *Leon*, 468 U.S. at 907 ("The substantial social costs exacted by the exclusionary rule for the vindication of Fourth Amendment rights have long been a source of concern."). It should not be lightly ordered if courts are to retain the respect of the public that is essential for them to carry out their duties.

For all of the foregoing reasons, the recommendation of Magistrate Judge Jones is adopted and Kienast's motion to suppress is denied. The Clerk is directed to place this matter on the Court's calendar for a change of plea or trial.

SO ORDERED at Green Bay, Wisconsin this 14th day of November, 2016.

s/ William C. Griesbach
William C. Griesbach, Chief Judge
United States District Court